

## REMARKS/ARGUMENTS

The amended listing of claims and the following arguments are presented generally to impart precision to the claims, by particularly pointing out and distinctly claiming the subject matter. The pending claims are supported by the specification. No new matter is added.

Claims 11 and 36 were objected to for informalities. The current amendment removes the informalities.

Claim 16 was rejected under 35 U.S.C. 112 for using the term “the received signal”. The current amendment eliminates the use of such a term from claim 16.

Claims 1-13, 16-17, 19-23 were rejected under 35 U.S.C. 102(b) as being anticipated by U.S. Patent No. 5,953,424 (hereinafter “Vogeleang”). Claims 14-15 and 18 were rejected under 35 U.S.C. 103(a) as being unpatentable over Vogeleang. Claims 24-41 were rejected under 35 U.S.C. 103(a) as being unpatentable over Vogeleang in view of U.S. Patent No. 5,666,415 (hereinafter “Kaufman”).

Applicant respectfully submits that the currently pending claims are patentable over the cited references.

For example, claim 1 recites:

1. (currently amended) A cryptographic method, including:  
receiving at a first entity a second public key  $M_A$ ;  
generating a first session key  $K_B$  based on the second public key  $M_A$ ;  
generating a first random nonce  $N_B$ ;  
encrypting the first random nonce  $N_B$  using at least a first password  $P_B$  and a first public key  $M_B$  to obtain an encrypted random nonce;  
transmitting the encrypted random nonce from the first entity;  
receiving a response to the encrypted random nonce; and  
authenticating through determining whether the response includes a correct modification of the first random nonce.

In Vogelesang, the public signal Y is received to generate the secrete S (Col. 16, lines 39-40, Vogelesang); and the private signal L is encrypted according to the secrete S (Col. 16, lines 64-65, Vogelesang). In Vogelesang, the private signal L is not encrypted using a password (e.g., KJ) and a public key (e.g., X). Thus, “*encrypting the first random nonce  $N_B$  using at least a first password  $P_B$  and a first public key  $M_B$  to obtain an encrypted random nonce*” is absent from Vogelesang. At least for this reason, Vogelesang does not anticipate claim 1.

Further, for example, claim 2 recites:

2. (currently amended) The method of claim 1 wherein said encrypting the first random nonce  $N_B$  includes:  
generating a first secrete  $S_B$  from at least the first password  $P_B$  and the first public key  $M_B$ ; and  
encrypting the first random nonce  $N_B$  using at least the first secrete  $S_B$ .

In Vogelesang, the first participant encrypts the private signal L according to the secrete S (Col. 16, lines 64-65, Vogelesang). The first participant of Vogelesang generates the secrete S from the public signal Y that is received from the second participant. However, the first participant of Vogelesang does not generate secrete from a password and another public signal (e.g., X, but not Y) to encrypt the private signal L. The secrete S of Vogelesang, which is considered as the session key and generated from Y (and KJ), is clearly different from “the first secrete  $S_B$ ” recited in claim 2. Thus, Vogelesang does not show “generating a first secrete  $S_B$  *from* at least *the first password  $P_B$  and the first public key  $M_B$* ” and “encrypting the first random nonce  $N_B$  using at least the first secrete  $S_B$ ”. Therefore, Vogelesang does not anticipate claim 2.

Further, for example, claim 16 recites:

16. (currently amended) The method of claim 2 wherein said transmitting the encrypted random nonce from the first entity includes:  
transmitting to a second entity the first public key  $M_B$  to establish the session key at the second entity; and  
wherein said authenticating includes:  
decrypting the response using the first session key  $K_B$  to generate a  
first decrypted result; and  
decrypting the first decrypted result using the first secret  $S_B$ .

In Vogelesang, the private signal  $L$  and the value  $T$  are encrypted according to the secrete  $S$  and transmitted from the first participant to the second participant. It is clear that in Vogelesang the transmission of the private signal  $L$  in the encrypted form does not include the transmission of the public signal (e.g.,  $X$ ) for the establishment of the session key (e.g.,  $S$  at the second participant). Since the generation of the value  $T$  of Vogelesang requires the decryption of  $Z_D$  using  $S$ , it is clear that the second participants is expected to have the secrete  $S$  before the private signal  $L$  is transmitted. Further, Thus, Vogelesang does not generate secrete using a public key that is transmitted to the second participant to establish the session key. Vogelesang does not anticipate claim 16.

Further, for example, claim 8 recites:

8. (currently amended) The method of claim 2 wherein said generating the first secrete  $S_B$  includes:  
combining the second public key  $M_A$  and the first public key  $M_B$  with the first password  $P_B$  to produce a first result, and  
hashing the first result with a secure hash.

In Vogelesang, there is no feature of “generating the first secrete  $S_B$ ”. Further, there is no feature of “combining the second public key  $M_A$  and the first public key  $M_B$  *with* the first

password  $P_B$  to produce a first result” in Vogelesang. Thus, Vogelesang does not anticipate claim 8.

Further, for example, claim 15 recites:

15. (currently amended) The method of claim 14, wherein superencrypting the first random nonce  $N_B$  includes:  
encrypting the first random nonce  $N_B$  with the first secret  $S_B$  to produce the first encrypted result; and  
encrypting the first encrypted result using the first session key  $K_B$ .

In Vogelesang, there is no feature of “generating the first secret  $S_B$ ”. Thus, in Vogelesang there is no “first encrypted result” that results from “encrypting the first random nonce  $N_B$  with the first secret  $S_B$ ”. In Vogelesang, the private signal  $L$  is only encrypted using the secret  $S$ , which is considered as a session key. The Office Action asserted that “the use of superencryption is not considered a novel feature”. Applicant respectfully disagrees. The Office Action did not show any evidence pointing a particular way of superencrypting as recited in the pending claims. Thus, claim 15 is neither anticipated by Vogelesang nor obvious in view of Vogelesang.

Further, for example, claim 17 recites:

17. (currently amended) The method of claim 2, wherein the response includes a combination of a second random nonce  $N_A$  and a modification of the first random nonce; and wherein the method further includes:  
extracting the second random nonce  $N_A$  from the response;  
modifying the second random nonce  $N_A$  to obtain a modified second random nonce;  
encrypting the modified second random nonce using the first session key  $K_B$  and the first secret  $S_B$  to obtain an encrypted package; and  
transmitting the encrypted package from the first entity.

In Vogelesang, the response to the private signal L is the value M, modified at the second participant and encrypted using the secret S. Thus, “second random nonce  $N_A$ ” is absent from the response to the private signal L of Vogelesang. Furthermore, the authentication process of Vogelesang ends when the correctness of M is verified. In Vogelesang (Col. 16, line 26 – Col. 17, line 38), the first participant is authenticated when the correctness of the value T is verified at the second participant (Col. 17, lines 1-19); and the second participant is authenticated when the correctness of the value M is verified at the first participant (Col. 17, lines 28-30). Vogelesang does not have the further operations of “extracting the second random nonce  $N_A$  ...”, “modifying the second random nonce  $N_A$  ...”, “encrypting the modified second random nonce ...”, and “transmitting the encrypted package ...”. Thus, Vogelesang does not anticipate claim 17.

Further, for example, claim 18 recites:

18. (currently amended) The method of claim 17 wherein said encrypting the modified second random nonce includes:  
generating a string of random bits  $I_B$ ;  
encrypting a combination of the string of random bits  $I_B$  and the modified second random nonce using the first secret  $S_B$  to generate a first result;  
and  
encrypting the first result using the first session key  $K_B$ .

Vogelesang does not have the further operation of “encrypting the modified second random nonce ...”, since the authentication process of Vogelesang ends when the correctness of M, as a response to the private signal L is verified. Furthermore, there is no “encrypting *a combination of the string of random bits  $I_B$  and the modified second random nonce* using the first secret  $S_B$  to generate a first result” and “encrypting the first result using the first session key  $K_B$ ”. Thus, Vogelesang does not anticipate claim 17.

In another aspect, for example, claim 24 recites:

24. (currently amended) A cryptographic method, comprising:  
receiving at a first entity a second public key  $M_A$  and an encrypted second random number;  
generating a first session key  $K_B$  based on the second public key  $M_A$ ;  
decrypting, using at least a first password  $P_B$  and the second public key  $M_A$ , to  
retrieve a second random number  $N_A$  from the encrypted second random number;  
modifying the second random number  $N_A$  to obtain a modified second random number;  
encrypting the modified second random number using at least the first  
password  $P_B$  and a first public key  $M_B$  to obtain an encrypted random  
package; and  
transmitting the encrypted random package from the first entity.

Applicant respectfully submits that a person skilled in the art would not reach a method as recited in claim 24 from the description of Vogelesang and Kaufman.

The Office Action asserted that “Kaufman describes an authentication similar to . Vogelesang’s in which a first entity, server, initially receives a password encrypted nonce.” Applicant respectfully disagrees.

According to Kaufman (Col. 3, lines 51-59), the server receives a first argument and a second argument. The first argument of Kaufman is a password of the user. The password is encrypted using a first one-way cryptographic transformation function for the first argument. The second argument includes an encrypted version of a combination of an encrypted version of the password and a nonce. According to Kaufman (Col. 4, lines 14-18), the second argument includes the nonce to defeat the attempt of an eavesdropper to replay previously recorded arguments.

From this description of Kaufman, a person skilled in the art understands that Kaufman and Vogelesang have dramatically different methods for authentication. In

Kaufman, the passwords of the users are transmitted over the network, in an encrypted form, for authentication. In Vogelesang, no password is transmitted for authentication. In Vogelesang, the secret information used for authentication (e.g., K and J) is not transmitted. The methods of Kaufman and Vogelesang are dramatically different. It is not apparent how the methods of Kaufman and Vogelesang might be combined and implemented with a reasonable expectation of success.

The Office Action asserted that "The password from a database is then used to obtain the random number." Applicant respectfully requests the examiner point out the particular description of either Kaufman or Vogelesang which supports such an assertion.

The Office Action relied upon Vogelesang (Col. 13, lines 41-67; Col. 14, lines 1-4) for a description of an authentication scheme which involves two nonces (L and V). However, applicant respectfully submits that Vogelesang describes the method of Col. 13, lines 41 – Col. 14, lines 4 to show the problems in this method. See, for example, Col. 14, lines 5-31. Thus, from the description of Vogelesang, a person skilled in the art understands that the method of Col. 13, lines 41 – Col. 14, lines 4 is a method separate from the method of Col. 16, lines 26 – Col. 17, lines 37. The method of Col. 16, lines 26 – Col. 17, lines 37 is proposed by Vogelesang to replace the method of Col. 13, lines 41 – Col. 14, lines 4, because of the problems as described in Col. 14, lines 5-31, Vogelesang.

Thus, applicant respectfully submits that it is improper to mix and match the elements of the method of Col. 13, lines 41 – Col. 14, lines 4 in Vogelesang with the method of Col. 16, lines 26 – Col. 17, lines 37 of Vogelesang. Here, one method is proposed to overcome the problems of another. It is not clearly why one would mix and match the methods.

Further, the combination of Vogelesang and Kaufman suggested in the Office Action is not proper. Kaufman does not show a random number encrypted by a password. Further, for the combination of Vogelesang and Kaufman suggested in the Office Action, the Office

Action did not point out a complete consistent method, which might be implementation with reasonable expectable of success.

Furthermore, neither Vogelesang nor Kaufman suggests “decrypting, *using at least a first password  $P_B$  and the second public key  $M_A$* , to retrieve a second random number  $N_A$  from the encrypted second random number” and “encrypting the modified second random number *using at least the first password  $P_B$  and a first public key  $M_B$*  to obtain an encrypted random package”.

Thus, at least for the above reasons, claim 24 is patentable over Vogelesang and Kaufman.

Further, for example, claims 25 and 34 recite additional limitations not found in Vogelesang and Kaufman.

25. (currently amended) The method of claim 24, wherein said decrypting includes:  
decrypting the encrypted second random number using the first session key  $K_B$  to generate a first decrypted result; and  
decrypting the first decrypted result using at least the first password  $P_B$  and the second public key  $M_A$ .
34. (currently amended) The method of claim 24, further including:  
generating a first random number  $N_B$ ; and  
wherein said encrypting the modified second random number includes:  
encrypting a combination of the first random number  $N_B$  and the modified second random number.

The remaining claims depend from at least one of the claims discussed above, or recite similar limitations discussed above, and therefore include at least some of the



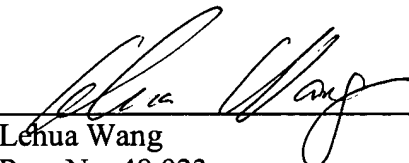
distinguishing claim limitations as discussed above. As a result, the remaining claims are also patentable.

Authorization is hereby given to charge our Deposit Account No. 02-2666 for any charges that may be due. Furthermore, if a further extension is required, Applicant hereby requests such extension.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN

Date: 5/13, 2005

  
\_\_\_\_\_  
Lehua Wang  
Reg. No. 48,023

12400 Wilshire Boulevard  
Seventh Floor  
Los Angeles, California 90025-1026  
(408) 720-8300